Solution 20

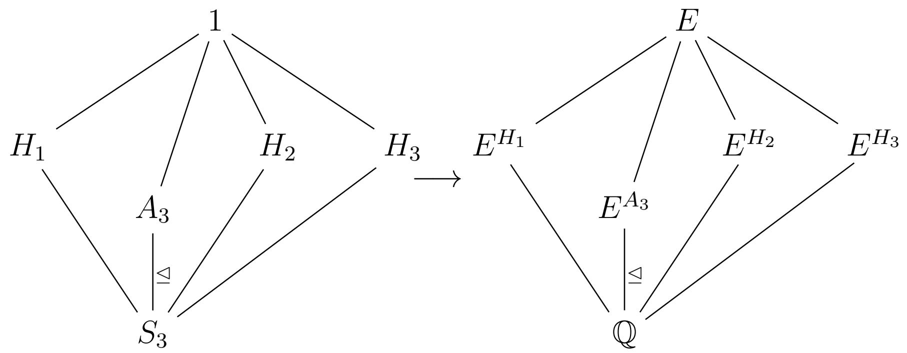
Galois correspondence. Simple extensions

1. Let $f = X^3 - 2 \in \mathbb{Q}[X]$ and consider its splitting field E. Recall from Assignment 16 that $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$. Write down the lattice of subgroups of S_3 and the corresponding fixed fields. Which of those are normal?

   Solution: The polynomial f has roots $z_1 = \sqrt[3]{2}$, $z_2 = \sqrt[3]{2}\omega$ and $z_3 = \sqrt[3]{2}\omega^2$, where $\omega = e^{\frac{2\pi i}{3}}$. The identification $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$ is given by $\sigma(z_i) = z_{\sigma(i)}$ for $\sigma \in S_3$. One can determine the image of ω under σ as

$$\sigma(\omega) = \frac{\sigma(z_2)}{\sigma(z_1)} = \frac{z_{\sigma(2)}}{z_{\sigma(1)}} = \omega^{\sigma(2)-\sigma(1)}.$$

   The subgroups of S_3 are given by 1, S_3 itself, $A_3 = \langle(1\ 2\ 3)\rangle$ and the three non-normal subgroups $H_i = \langle(j\ k)\rangle$ for each choice of $\{i, j, k\} = \{1, 2, 3\}$. The only containments are given by $1 \leqslant H_i \leqslant S_3$ and $1 \leqslant A_3 \trianglelefteq S_3$. Denoting by E^G the fixed field of G, we have



   By construction, we see that H_i fixes z_i for each $i \in \{1, 2, 3\}$, so that $\mathbb{Q}(z_i) \subset E^{H_i}$. Since $[E : \mathbb{Q}(z_i)] = 2 = |H_i| = [E : E^{H_i}]$, we conclude that $E^{H_i} = \mathbb{Q}(z_i)$.

   By Galois correspondence, $E^{A_3}/\mathbb{Q}$ is the only intermediate extension which is Galois, and it is also the unique extension of degree 2. Since $\mathbb{Q}(\omega)/\mathbb{Q}$ is a quadratic field extension (the minimal polynomial of ω being $X^2 + X + 1 \in \mathbb{Q}[X]$) and $\mathbb{Q}(\omega) \subset E$, we must have $E^{A_3} = \mathbb{Q}(\omega)$. Alternatively, one can directly check that A_3 fixes ω and conclude by comparing the degrees of the extensions: For $\tau = (1\ 2\ 3)$, a generator of A_3, we have

$$\tau(\omega) = \omega^{\tau(2)-\tau(1)} = \omega^{3-2} = \omega.$$

2. Let k be a field and $f \in k[X]$ a polynomial with distinct roots. Let E be the splitting field of f and enumerate the roots of f by $z_1, \ldots, z_n$ to fix an embedding $\mathrm{Gal}(E/k) \subset S_n$. Define the discriminant of f as

$$D(f) = \prod_{i<j} (z_i - z_j)^2.$$

   (a) Assume that $\mathrm{char}(k) \neq 2$. Prove that $D(f)$ is a square in k if and only if $\mathrm{Gal}(E/k) \subset A_n$.

   (b) Show that $\mathbb{F}_4/\mathbb{F}_2$ is a counterexample in characteristic 2 to the previous part.

   Solution:

   (a) Let $\Delta(f) = \prod_{i<j}(z_i - z_j)$. The square roots of $D(f)$ in E are given by $\pm\Delta(f)$, so $D(f)$ is a square in k if and only if $\Delta(f) \in k$. For $\sigma \in \mathrm{Gal}(E/k)$, we have $\sigma(\Delta(f)) = \mathrm{sgn}(\sigma)\Delta(f)$ (since the z_i are distinct); hence $\Delta(f)$ is fixed by σ if and only if $\sigma \in A_n$ (because $\mathrm{char}(k) \neq 2$).

   Since E/k is Galois, $\Delta(f)$ lies in k if and only if it is fixed by all $\sigma \in \mathrm{Gal}(E/k)$, which by what we just showed is equivalent to $\mathrm{Gal}(E/k) \subset A_n$.

   (b) For $k = \mathbb{F}_2$ and $E = \mathbb{F}_4$, we have $\mathrm{Gal}(E/k) = S_2 = \langle\sigma\rangle$, where σ is the Frobenius automorphism of $\mathbb{F}_4$. We can write $E = k(\alpha)$ where α is a root of $f = X^2 + X + 1 \in k[X]$, and E is a splitting field of f. The other root of f is $\alpha + 1$. Then $\Delta(f) = (\alpha + 1) - \alpha = 1 \in \mathbb{F}_2$, so that $D(f)$ is a square in $\mathbb{F}_2$, although $\mathrm{Gal}(E/k)$ is not contained in $A_2 = 1$.

3. Let L/k be a finite field extension and fix an embedding $L \subset \overline{k}$.

   (a) Show that there exists a minimal finite field extension E/k containing L which is the splitting field of some polynomial.

   (b) Show that if L/k is separable (i.e. the minimal polynomial over k of any element in L has distinct roots in $\bar{k}$), then E/k is Galois. In this case, E is called the *Galois closure of L/k*.

   Hint: Assignment 19, Exercise 3.

   Solution:

(a) Since L/k is a finite extension, it is finitely generated. Write $L = k(x_1, \dots, x_n)$ and for each $i = 1, \dots, n$ let f_i be the minimal polynomial of x_i over k. Let E be the splitting field of the product $f = f_1 \cdots f_n$. Then E clearly contains L. By Assignment 19, Exercise 3(a), we know that any extension of k which is the splitting field of some polynomial $g \in k[X]$ and contains x_i must contain all roots of its minimal polynomial f_i as well, so E is minimal by construction.

(b) If L/k is separable, then E/k from Part (a) is the splitting field of a polynomial with distinct roots as shown in the proof of Part (b) of Exercise 3 in Assignment 19. Thus, again by that exercise, E/k is Galois.

4. We say that a field extension L/k is *simple* if there exists $x \in L$ such that $L = k(x)$. In this exercise we will prove the following result:

Lemma. A finite field extensions L/k is simple if and only if there are finitely many intermediate field extensions $L/F/k$.

(a) Suppose $L = k(x)$ for some $x \in L$ and let $L/F/k$ be an intermediate extension. Let $f \in F[X]$ be the minimal polynomial of x over F and let $F_0 \subset F$ be the extension of k generated by the coefficients of f. Prove that $F = F_0$.

Hint: Check that $F(x) = F_0(x)$ and compare degrees.

(b) Conclude that if L/k is simple, then it contains only finitely many intermediate subextensions.

Hint: In Part (a), f divides the minimal polynomial of x over k.

(c) Let k be an infinite field and V a k-vector space. Suppose that $V_1, \dots, V_m$ are finitely many proper subspaces of V. Prove by induction that $\bigcup_{i=1}^m V_i \neq V$.

(d) Suppose that a finite field extension L/k contains only finitely many intermediate extensions. Prove that L/k is simple.

Solution:

(a) The polynomial f is irreducible in $F[X]$, hence also in $F_0[X]$. This means that $[F(x) : F] = \deg(f) = [F_0(x) : F_0]$. But

$$L = k(x) \subset F_0(x) \subset F(x) \subset L$$

implies that $F_0(x) = F(x)$, so that

$$[F : F_0] = \frac{[F(x) : F_0]}{[F(x) : F]} = \frac{[F_0(x) : F_0]}{[F(x) : F]} = 1.$$

(b) By Part (a), if $L = k(x)/F/k$ is an intermediate extension, then F is generated by the coefficients of the minimal polynomial f of x over F, which is a proper monic factor of the minimal polynomial g of x over k in $L[X]$. Since g has only finitely many proper monic factors, there are only finitely many intermediate extensions $L/F/k$.

(c) See Chambert-Loir, *A Field Guide to Algebra*, Lemma 3.3.4.

(d) Suppose that k is finite. Then L is finite, too. By Algebra I, we know that $L^\times$ is a cyclic group, so that for x a generator of $L^\times$, we know that $k(x)$ contains the whole $L^\times$, implying that $L = k(x)$.

Suppose that k is an infinite field. By assumption, there are only finitely many intermediate extensions of L/k. In particular, there are only finitely many intermediate *simple* extensions $L_1, \ldots, L_m/k$. As each $u \in L$ lies in the simple extension $k(u)$, we know that $L = \cup_{i=1}^m L_i$. Then, by Part (c), we must have $L = L_i$ for some i, so L/k is itself a simple extension.

5. (*Primitive Element Theorem*) Let L/k be a finite separable field extension. Prove that there exists $x \in L$ such that $L = k(x)$, i.e. that L is simple.

Hint: Use the preceding exercises.

Solution: By Exercise 3, L/k is contained in a finite Galois extension E/k. By the Galois correspondence, the intermediate field extensions of E/k are in bijection with the subgroups of the finite group $\mathrm{Gal}(E/k)$, so there are only finitely many. This implies that L/k also has only finitely many intermediate field extensions. By Exercise 4, L/k is a simple extension.

6. Prove that the field extension $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$, where s and t are formal variables, contains infinitely many intermediate extensions.

Hint: Use Exercise 4.

Solution: By Exercise 4, it suffices to prove that $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$ is not simple. We first compute the degree of this extension. We have a tower of field extensions $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t)/\mathbb{F}_p(s^p,t^p)$. Note that $\mathbb{F}_p(s,t) = \mathbb{F}_p(s^p,t)(s)$ and that s is the unique root of the polynomial

$$(X-s)^p = X^p - s^p \in \mathbb{F}_p(s^p,t)[X],$$

which is irreducible because its monic proper factors in $\mathbb{F}_p(s,t)[X]$ have constant term not in $\mathbb{F}_p(s^p,t)$. Thus, we obtain $[\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t)] = p$. Similarly, we see that $[\mathbb{F}_p(s^p,t) : \mathbb{F}_p(s^p,t^p)] = p$ because $X^p - t^p$ is the minimal polynomial of t over $\mathbb{F}_p(s^p,t^p)$. All in all we obtain

$$[\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t^p)] = [\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t)][\mathbb{F}_p(s^p,t) : \mathbb{F}_p(s^p,t^p)] = p^2.$$

Suppose by contradiction that $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$ is simple and let $f \in \mathbb{F}_p(s,t)$ be a generator, i.e. $\mathbb{F}_p(s,t) = \mathbb{F}_p(s^p,t^p)(f)$. The Frobenius map $x \mapsto x^p$ is a field endomorphism of $\mathbb{F}_p(s,t)$, which implies that $f^p \in \mathbb{F}_p(s^p,t^p)$. Thus, the minimal polynomial of f over $\mathbb{F}_p(s^p,t^p)$ divides $X^p - f^p \in \mathbb{F}_p(s^p,t^p)[X]$, so

$$p^2 = [\mathbb{F}_p(s,t) : \mathbb{F}_p(s^p,t^p)] = [\mathbb{F}_p(s^p,t^p)(f) : \mathbb{F}_p(s^p,t^p)] \leqslant p,$$

a contradiction. Hence $\mathbb{F}_p(s,t)/\mathbb{F}_p(s^p,t^p)$ is not simple.